U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office

DOCUMENT RETRIEVAL REQUEST FORM

Requester's Name: Chad Zhong	Case Serial Number: 09/614,867		Art Unit/Org.: 2154
Phone: 305-0718	Fax:	Building: CPK-2	Room Number: 04R09
Class/Sub-Class: 709 - 203			
Date of Request: 8/26/03		Date Needed By: 8/26/03	

Paste or add text of citation or bibliography: **Paste Citation** Only one request per form. Original copy only. ☐

Author/Editor:	
Journal/Book Title:	
Article Title:	
Volume Number:	Report Number: Pages:
Issue Number:	Series Number: Year of Publication:
Publisher:	
Remarks: 253	See attached

Staff Use Only

Monthly Accession Number:

Library Action	PTO		LC		NAL		NIH		NLM		NIST		Other	
	1st	2nd	1st	2nd	1st	2nd	1st	2nd	1st	2nd	1st	2nd	1st	2nd
Local Attempts	✓													
Date	8/27													
Initials	nd													
Results	Copy													
Examiner Called												✓		
Page Count														
Money Spent														

	Source	Date
Remarks/Comments 1st and 2nd denotes time taken to a library O/N – Under NLM means Overnight	**Ordered From:**	

Comments:

f your web server, the browser uses Windows NT Challenge/Response chentication.

In general, all updates and **security** fixes to IIS should be installed before the web server is made available. You can find the...

...Microsoft web site (http://wwwmicrosoft.com/). For more information on securing your web server, see the "WWW **Service** Registry Entries" and "Securing Your Site Against Intruders" topics in online help for Microsoft Internet Information Server probably need to do more research on each topic to ensure that you have the appropriate **security** settings for your particular application needs. The Microsoft web site has a complete section on **security** , which can be found at http://wwwmicrosoft.com/ **security** /.

Conclusion

Security in a connected and information-intensive environment is critical to the success of the Web as a...

...COMPANY NAMES: **Products**
DESCRIPTORS: Network **Security** Software...

...Internet **Security**

11/5,K/5 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

02074418 SUPPLIER NUMBER: 19520428 (USE FORMAT 7 OR 9 FOR FULL TEXT)
C is for cookie . **(includes related article on tips, tricks and techniques) (Internet Expert) (Internet/Web/Online** Service **Information) (Brief Article)**
Bott, Ed
PC/Computing, v10, n7, p324(1)
July, 1997
DOCUMENT TYPE: Brief Article ISSN: 0899-1847 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 1441 LINE COUNT: 00119

SPECIAL FEATURES: illustration; other
DESCRIPTORS: Internet/Web Technology; Privacy Issue
FILE SEGMENT: CD File 275

C is for cookie . **(includes related article on tips, tricks and techniques) (Internet Expert) (Internet/Web/Online** Service **Information) (Brief Article)**

TEXT:

Every time you click on a link in your Web browser there's a **good** chance you'll get more than you asked for. A hidden chunk of data called a " **cookie** " could hitchhike down the wire along with the data you requested and plant itself on your hard...

...all perfectly legal, but some privacy advocates are justifiably concerned about the amount of personal information that **cookies** can give away.

In more formal circles, **cookies** are called client-side persistent data, and they offer a simple and generally secure way for a Web server to keep track of a user's actions. There are dozens of legitimate applications for **cookies** : Commercial Web sites use them to remember items in a visitor's shopping basket; information providers store usernames and passwords; search engines record your preferences. A Web site can also use **cookies** to create a profile of your browsing habits, based on pages you've visited or information you've entered in a Web-based form.

The first time you access a **cookie** -enabled server from a compatible Web browser, the server creates a new record in your **cookie** collection. That record contains the server's domain name, an expiration date, some **security** information, and any information the Web designer chooses to store about the current page request. When you...

02074418 SUPPLIER NUMBER: 19520428 (THIS IS THE FULL TEXT)

C is for cookie. (includes related article on tips, tricks and techniques) (Internet Expert) (Internet/Web/Online Service Information) (Brief Article)

Bott, Ed

PC/Computing , v10, n7, p324(1)
July, 1997
DOCUMENT TYPE: Brief Article ISSN: 0899-1847 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 1441 LINE COUNT: 00119

TEXT:

Every time you click on a link in your Web browser there's a good chance you'll get more than you asked for. A hidden chunk of data called a "cookie" could hitchhike down the wire along with the data you requested and plant itself on your hard drive, without your knowledge. It's all perfectly legal, but some privacy advocates are justifiably concerned about the amount of personal information that cookies can give away.

In more formal circles, cookies are called client-side persistent data, and they offer a simple and generally secure way for a Web server to keep track of a user's actions. There are dozens of legitimate applications for cookies: Commercial Web sites use them to remember items in a visitor's shopping basket; information providers store usernames and passwords; search engines record your preferences. A Web site can also use cookies to create a profile of your browsing habits, based on pages you've visited or information you've entered in a Web-based form.

The first time you access a cookie-enabled server from a compatible Web browser, the server creates a new record in your cookie collection. That record contains the server's domain name, an expiration date, some security information, and any information the Web designer chooses to store about the current page request. When you revisit that page (or access another page on the same site), the server reads and updates information in the cookie record.

There are strict security controls over what a Web server can and cannot do with cookies. They can't be used to retrieve information from your hard disk or your network. Also, a server can retrieve information only from a cookie that it or another server in its domain created. A cookie can track your movements only within a given site--it can't tell a server where you came from or where you're going next. The data in cookies is usually encoded, so it would be useless to a data thief.

Netscape Navigator versions 2.0 and later support cookies, as does Microsoft Internet Explorer 3.0. Both leading browsers also offer limited tools for managing cookies. But exercising tight control over the information stored in cookies requires third-party software.

Related Article: Tips, Tricks, and Techniques

What's in that cookie file?

Before you can peek in a cookie file, you have to know where to look. On Windows machines, Netscape Navigator tracks cookie information in a text file called Cookies.txt; you'll find it in the same folder as the Netscape Program files. Microsoft Internet Explorer 3.0 creates a Cookies folder inside the Windows folder, then stores each cookie there as a separate text file. In either case, a cookie is no more than 4K in size. Although you can open any cookie file with Notepad or another text editor, you'll be unable to make sense of the contents. The name of the domain that set the cookie is in clear text, but most other entries are encoded as numeric strings that are meaningless without a key.

Tell Navigator and Internet Explorer to alert you when cookies arrive.

Both leading Web browsers offer a feature that pops up a dialog box each time a Web server attempts to set a cookie. You can accept or reject the offer, and many cookie-enabled Web sites--especially those that are simply tracking advertising statistics--still work when you say no. Navigator users: Choose Options, then Network Preferences, click on the Protocols tab, and check the box labeled Show an Alert Before Accepting a Cookie. Internet Explorer 3.0 users: Choose View, then Options, click on the Advanced tab, and check the box labeled Warn Before Accepting "Cookies." If you choose to be notified, prepare to be annoyed. Some popular sites add or update a cookie every time you click, and the extra dialog boxes become maddening.

Don't be too quick to zap those cookie files.

Some online advisors suggest deleting cookie collections to safeguard personal data. But certain sites store useful information in cookies, and killing cookie files can make those sites far less user-friendly. The online New York Times (www.nytimes.com), for example, caches your password and username in a cookie file; delete that entry and you'll need to log in every time you visit the site. Netscape (personal.netscape.com/custom) and Microsoft (home.microsoft.com/personalizing/personalizing.asp) use cookies to create customized home pages for you; if those cookies disappear, so does your custom home page.

Lock up your cookies.

Navigator users can preserve existing cookie information but lock out any changes or additions by setting their cookie file to read-only. (In the Windows Explorer, right-click on Cookies.txt, choose Properties, and check the Read-Only box.) Now whenever you browse, cookie information is stored in memory, so you can still conduct online shopping sessions. The information is not saved when you exit, however. Because Microsoft's browser uses individual cookie files, there's no equivalent option for Internet Explorer 3.0 users. Although some articles suggest you can disable cookies for an individual domain by corrupting its entry in the Cookies folder, then setting the file's attributes to read-only, this technique is a hassle, doesn't work consistently, and might cause your browser to crash.

Who uses cookies? Find out online.

Robert Brooks's Cookie Taste Test page (www.geocities.com/SoHo/4535/cookie.html) includes a list of well-known sites that use cookies. Not surprisingly, Microsoft made the list, as did Intel, Progressive Networks (makers of RealAudio software), disney.com, and several popular Internet search engines. If you know of a site that uses cookies, use the online form here to add a new entry to the collection.

If you don't like the way a site uses cookies, let the Webmaster know.

Some sites have a legitimate need to use cookies, but others pepper users with new cookies every time they click on a hyperlink, for no good reason. If you want to know what kind of information is stored in a specific cookie file, send an email to the Webmaster of the site that set the cookie. You may be surprised by the response: Some Web-server software sets cookies by default, and a politely worded query may be sufficient to convince the Webmaster to turn off cookies.

Essential Cookie Resources

The Tools The Lowdown

Center for Democracy and Technology Privacy Demonstration Page
www.cdt.org/privacy/

Who's watching you and what are you telling them? Check out this compelling demonstration of the type of information Web sites can discover about visitors. Also, there's news, discussions, and demonstrations of Internet-related privacy issues, as well as the political and legal issues surrounding cookies.

Cookie Central
www.cookiecentral.com

Here's an amusing, informative, and thoroughly entertaining look at cookies, with great links and a well-balanced perspective. Plus, complete information on persistent cookies, HTTP cookies, cookies with JavaScript, and the dark side of cookies.

Cookie Crusher
www6.zdnet.com/cgi-bin/texis/swlib/hotfiles/info.html?fcode=000DUV

Automatically and silently rejects cookies so they are not saved to your hard drive, eliminating potential privacy and security violations. Unfortunately, The setup is needlessly difficult, and you first have to set Microsoft Internet Explorer's or Netscape Navigator's cookie-alert option, after which you briefly see cookie dialog boxes before Cookie Crusher makes them go away. Available for a $10 shareware fee.

NSClean and IEClean
www.wizvax.net/kevinmca/

Shows you what information your browser records about who you are, where you've been, and what you've seen. This pro-privacy software then

lets you change or delete it. But despite the alarmist hype, NSClean and IEClean generally work as advertised, letting you view and delete information in cookies and much more. Pick these up for a $30 to $40 shareware fee.

Persistent Client State HTTP Cookies
www.netscape.com/newsref/std/cookie_spec.html

Solid technical explanations of cookies, although content is directed heavily toward developers. While you will find a general overview, specifications, and example scripts for cookies, you won't find discussions of the moral and legal issues involved.

ZDNet's CookieMaster
www6.zdnet.com/cgi-bin/texis/swlib/hotfiles/info.html?fcode=000CKP

A quick and easy way to monitor cookie activity on your computer. CookieMaster adds an icon to the right side of your Taskbar that pops up a list of cookies; deleting the ones you don't want is simple. Plus it's compatible with both Navigator and Internet Explorer. If you surf a lot of cookie sites, you'll appreciate CookieMaster.

SPECIAL FEATURES: illustration; other
DESCRIPTORS: Internet/Web Technology; Privacy Issue
FILE SEGMENT: CD File 275

page (or access another page on the same site), the server reads and updates information in the **cookie** record.

There are strict **security** controls over what a Web server can and cannot do with **cookies** . They can't be used to retrieve information from your hard disk or your network. Also, a server can retrieve information only from a **cookie** that it or another server in its domain created. A **cookie** can track your movements only within a given site--it can't tell a server where you came from or where you're going next. The data in **cookies** is usually encoded, so it would be useless to a data thief.

Netscape Navigator versions 2.0 and later support **cookies** , as does Microsoft Internet Explorer 3.0. Both leading browsers also offer limited tools for managing **cookies** . But exercising tight control over the information stored in **cookies** requires **third - party** software.

Related Article: Tips, Tricks, and Techniques

What's in that **cookie** file?

Before you can peek in a **cookie** file, you have to know where to look. On Windows machines, Netscape Navigator tracks **cookie** information in a text file called **Cookies** .txt; you'll find it in the same folder as the Netscape Program files. Microsoft Internet Explorer 3.0 creates a **Cookies** folder inside the Windows folder, then stores each **cookie** there as a separate text file. In either case, a **cookie** is no more than 4K in size. Although you can open any **cookie** file with Notepad or another text editor, you'll be unable to make sense of the contents. The name of the domain that set the **cookie** is in clear text, but most other entries are encoded as numeric strings that are meaningless without a key.

Tell Navigator and Internet Explorer to alert you when **cookies** arrive.

Both leading Web browsers offer a feature that pops up a dialog box each time a Web server attempts to set a **cookie** . You can accept or reject the offer, and many **cookie** -enabled Web sites--especially those that are simply tracking advertising statistics--still work when you say no...

...Preferences, click on the Protocols tab, and check the box labeled Show an Alert Before Accepting a **Cookie** . Internet Explorer 3.0 users: Choose View, then Options, click on the Advanced tab, and check the box labeled Warn Before Accepting " **Cookies** ." If you choose to be notified, prepare to be annoyed. Some popular sites add or update a **cookie** every time you click, and the extra dialog boxes become maddening.

Don't be too quick to zap those **cookie** files.

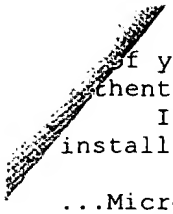
Some online advisors suggest deleting **cookie** collections to **safeguard** personal data. But certain sites store useful information in **cookies** , and killing **cookie** files can make those sites far less user-friendly. The online New York Times (www.nytimes.com), for example, caches your password and username in a **cookie** file; delete that entry and you'll need to log in every time you visit the site. Netscape (personal.netscape.com/custom) and Microsoft (home.microsoft.com/personalizing/personalizing.asp) use **cookies** to create customized home pages for you; if those **cookies** disappear, so does your custom home page.

Lock up your **cookies** .

Navigator users can preserve existing **cookie** information but lock out any changes or additions by setting their **cookie** file to **read** -only. (In the Windows Explorer, right-click on **Cookies** .txt, choose Properties, and check the **Read** -Only box.) Now whenever you browse, **cookie** information is stored in memory, so you can still conduct online shopping sessions. The information is not saved when you exit, however. Because Microsoft's browser uses individual **cookie** files, there's no equivalent option for Internet Explorer 3.0 users. Although some articles suggest you can disable **cookies** for an individual domain by corrupting its entry in the **Cookies** folder, then setting the file's attributes to **read** -only, this technique is a hassle, doesn't work consistently, and might cause your browser to crash.

Who uses **cookies** ? Find out online.

Robert Brooks's **Cookie** Taste Test page (www.geocities.com/SoHo/4535/**cookie** .html) includes a list of well-known sites that use **cookies** . Not surprisingly, Microsoft made the list, as did Intel, Progressive Networks



f your web server, the browser uses Windows NT Challenge/Response thentication.

In general, all updates and **security** fixes to IIS should be installed before the web server is made available. You can find the...

...Microsoft web site (http://wwwmicrosoft.com/). For more information on securing your web server, see the "WWW **Service** Registry Entries" and "Securing Your Site Against Intruders" topics in online help for Microsoft Internet Information Server probably need to do more research on each topic to ensure that you have the appropriate **security** settings for your particular application needs. The Microsoft web site has a complete section on **security** , which can be found at http://wwwmicrosoft.com/ **security** /.

Conclusion

Security in a connected and information-intensive environment is critical to the success of the Web as a...

...COMPANY NAMES: **Products**
DESCRIPTORS: Network **Security** Software...

...Internet **Security**

11/5,K/5 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

02074418 SUPPLIER NUMBER: 19520428 (USE FORMAT 7 OR 9 FOR FULL TEXT)
C is for cookie . **(includes related article on tips, tricks and techniques) (Internet Expert) (Internet/Web/Online** Service **Information) (Brief Article)**
Bott, Ed
PC/Computing, v10, n7, p324(1)
July, 1997
DOCUMENT TYPE: Brief Article ISSN: 0899-1847 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 1441 LINE COUNT: 00119

SPECIAL FEATURES: illustration; other
DESCRIPTORS: Internet/Web Technology; Privacy Issue
FILE SEGMENT: CD File 275

C is for cookie . **(includes related article on tips, tricks and techniques) (Internet Expert) (Internet/Web/Online** Service **Information) (Brief Article)**

TEXT:

Every time you click on a link in your Web browser there's a **good** chance you'll get more than you asked for. A hidden chunk of data called a " **cookie** " could hitchhike down the wire along with the data you requested and plant itself on your hard...

...all perfectly legal, but some privacy advocates are justifiably concerned about the amount of personal information that **cookies** can give away.

In more formal circles, **cookies** are called client-side persistent data, and they offer a simple and generally secure way for a Web server to keep track of a user's actions. There are dozens of legitimate applications for **cookies** : Commercial Web sites use them to remember items in a visitor's shopping basket; information providers store usernames and passwords; search engines record your preferences. A Web site can also use **cookies** to create a profile of your browsing habits, based on pages you've visited or information you've entered in a Web-based form.

The first time you access a **cookie** -enabled server from a compatible Web browser, the server creates a new record in your **cookie** collection. That record contains the server's domain name, an expiration date, some **security** information, and any information the Web designer chooses to store about the current page request. When you...

page (or access another page on the same site), the server reads and updates information in the **cookie** record.

There are strict **security** controls over what a Web server can and cannot do with **cookies** . They can't be used to retrieve information from your hard disk or your network. Also, a server can retrieve information only from a **cookie** that it or another server in its domain created. A **cookie** can track your movements only within a given site--it can't tell a server where you came from or where you're going next. The data in **cookies** is usually encoded, so it would be useless to a data thief.

Netscape Navigator versions 2.0 and later support **cookies** , as does Microsoft Internet Explorer 3.0. Both leading browsers also offer limited tools for managing **cookies** . But exercising tight control over the information stored in **cookies** requires **third** - **party** software.

Related Article: Tips, Tricks, and Techniques

What's in that **cookie** file?

Before you can peek in a **cookie** file, you have to know where to look. On Windows machines, Netscape Navigator tracks **cookie** information in a text file called **Cookies** .txt; you'll find it in the same folder as the Netscape Program files. Microsoft Internet Explorer 3.0 creates a **Cookies** folder inside the Windows folder, then stores each **cookie** there as a separate text file. In either case, a **cookie** is no more than 4K in size. Although you can open any **cookie** file with Notepad or another text editor, you'll be unable to make sense of the contents. The name of the domain that set the **cookie** is in clear text, but most other entries are encoded as numeric strings that are meaningless without a key.

Tell Navigator and Internet Explorer to alert you when **cookies** arrive.

Both leading Web browsers offer a feature that pops up a dialog box each time a Web server attempts to set a **cookie** . You can accept or reject the offer, and many **cookie** -enabled Web sites--especially those that are simply tracking advertising statistics--still work when you say no...

...Preferences, click on the Protocols tab, and check the box labeled Show an Alert Before Accepting a **Cookie** . Internet Explorer 3.0 users: Choose View, then Options, click on the Advanced tab, and check the box labeled Warn Before Accepting " **Cookies** ." If you choose to be notified, prepare to be annoyed. Some popular sites add or update a **cookie** every time you click, and the extra dialog boxes become maddening.

Don't be too quick to zap those **cookie** files.

Some online advisors suggest deleting **cookie** collections to **safeguard** personal data. But certain sites store useful information in **cookies** , and killing **cookie** files can make those sites far less user-friendly. The online New York Times (www.nytimes.com), for example, caches your password and username in a **cookie** file; delete that entry and you'll need to log in every time you visit the site. Netscape (personal.netscape.com/custom) and Microsoft (home.microsoft.com/personalizing/personalizing.asp) use **cookies** to create customized home pages for you; if those **cookies** disappear, so does your custom home page.

Lock up your **cookies** .

Navigator users can preserve existing **cookie** information but lock out any changes or additions by setting their **cookie** file to **read** -only. (In the Windows Explorer, right-click on **Cookies** .txt, choose Properties, and check the **Read** -Only box.) Now whenever you browse, **cookie** information is stored in memory, so you can still conduct online shopping sessions. The information is not saved when you exit, however. Because Microsoft's browser uses individual **cookie** files, there's no equivalent option for Internet Explorer 3.0 users. Although some articles suggest you can disable **cookies** for an individual domain by corrupting its entry in the **Cookies** folder, then setting the file's attributes to **read** -only, this technique is a hassle, doesn't work consistently, and might cause your browser to crash.

Who uses **cookies** ? Find out online.

Robert Brooks's **Cookie** Taste Test page (www.geocities.com/SoHo/4535/**cookie** .html) includes a list of well-known sites that use **cookies** . Not surprisingly, Microsoft made the list, as did Intel, Progressive Networks

kers of RealAudio software), disney.com, and several popular Internet arch engines. If you know of a site that uses **cookies** , use the online form here to add a new entry to the collection.

If you don't like the way a site uses **cookies** , let the Webmaster know.

Some sites have a legitimate need to use **cookies** , but others pepper users with new **cookies** every time they click on a hyperlink, for no **good** reason. If you want to know what kind of information is stored in a specific **cookie** file, send an email to the Webmaster of the site that set the **cookie** . You may be surprised by the response: Some Web-server software sets **cookies** by default, and a politely worded query may be sufficient to convince the Webmaster to turn off **cookies** .

Essential **Cookie** Resources

The Tools The Lowdown

Center for Democracy and Technology Privacy Demonstration Page

www.cdt.org/privacy...

...discussions, and demonstrations of Internet-related privacy issues, as well as the political and legal issues surrounding **cookies** .

Cookie Central

www. **cookiecentral** .com

Here's an amusing, informative, and thoroughly entertaining look at **cookies** , with great links and a well-balanced perspective. Plus, complete information on persistent **cookies** , HTTP **cookies** , **cookies** with JavaScript, and the dark side of **cookies** .

Cookie Crusher

www6.zdnet.com/cgi-bin/texis/swlib/hotfiles/info.html?fcode=000DUV

Automatically and silently rejects **cookies** so they are not saved to your hard drive, eliminating potential privacy and **security** violations. Unfortunately, The setup is needlessly difficult, and you first have to set Microsoft Internet Explorer's or Netscape Navigator's **cookie** -alert option, after which you briefly see **cookie** dialog boxes before **Cookie** Crusher makes them go away. Available for a $10 shareware fee.

NSClean and IEClean

www.wizvax.net...

...the alarmist hype, NSClean and IEClean generally work as advertised, letting you view and delete information in **cookies** and much more. Pick these up for a $30 to $40 shareware fee.

Persistent Client State HTTP **Cookies**

www.netscape.com/newsref/std/ **cookie** _...

...spec.html

Solid technical explanations of **cookies** , although content is directed heavily toward developers. While you will find a general overview, specifications, and example scripts for **cookies** , you won't find discussions of the moral and legal issues involved.

ZDNet's **CookieMaster**

www6.zdnet.com/cgi-bin/texis/swlib/hotfiles/info.html?fcode=000CKP

A quick and easy way to monitor **cookie** activity on your computer. **CookieMaster** adds an icon to the right side of your Taskbar that pops up a list of **cookies** ; deleting the ones you don't want is simple. Plus it's compatible with both Navigator and Internet Explorer. If you surf a lot of **cookie** sites, you'll appreciate **CookieMaster** .

11/5,K/6 (Item 6 from file: 275)

02055167 SUPPLIER NUMBER: 19308334 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Tasty cookies , **without guilt. (includes related articles on expert tips, concealing** cookies **) (Internet/Web/Online** Service **Information)**